CYBERSECURITY (CYBR)

CYBR 1100 INTRODUCTION TO INFORMATION SECURITY (3 credits)
This course emphasizes our current dependence on information technology and how its security in cyberspace (or lack thereof) is shaping the global landscape. Several historical and contemporary global events that have been influenced by the exploitation of information technology motivates topics on cyber crime, malware, intrusion detection, cryptography, among others, and how to secure one’s own data and computer system. Several aspects of this course are geared towards developing an understanding of the "cyberspace" as a new medium that breaks all geographical boundaries, while highlighting noticeable influences on it from social, political, economic and cultural factors of a geographical region.

Distribution: Global Diversity General Education course

CYBR 2250 LOW-LEVEL PROGRAMMING (3 credits)
This course will teach the cybersecurity students low-level programming in the 'C' and assembly languages, and the interrelationship between these two programming paradigms. The student will learn the various control structures in 'C' and how they are implemented in machine code, memory allocation and management, and the basics of allocation classes such as static versus automatic variables. The students will also learn x86 assembly language in the 'C' environment and will be able to write useful, functional, stand-alone assembly language programs with no help from external libraries.

Prerequisite(s)/Corequisite(s): CSCI 1620. Not open to non-degree graduate students.

CYBR 2980 SPECIAL TOPICS IN INFORMATION ASSURANCE (1-3 credits)
The course provides a format for exploring subject areas in Information Assurance and related fields for sophomore undergraduate students. Specific topics vary, in keeping with research interests of faculty and students. Examples include network configuration, network security, forensics, regulatory compliance, web services and applications, vulnerability assessments, cloud computing security, and other issues in Information Assurance.

Prerequisite(s)/Corequisite(s): Instructor permission required. Not open to non-degree graduate students.

CYBR 3250 SECURITY ADMINISTRATION - LINUX (3 credits)
This course covers topics a system administrator would encounter in their profession. The student will learn how a system administrator fulfills various organizational information resource management requirements using the a Linux-based Operating System. Topics will include; installation; creating and maintaining file systems; user and group administration; backup and restore processes; network configuration; various system services; simple security administration; and updating and maintaining the system.

Prerequisite(s)/Corequisite(s): CSCI 1620 or CSCI 1840 or Instructor Permission.

CYBR 3350 SECURITY ADMINISTRATION - LINUX (3 credits)
This course covers topics a system administrator would encounter in their profession. The student will learn how a system administrator fulfills various organizational information resource management requirements using the Linux-based Operating System. Topics will include; installation; creating and maintaining file systems; user and group administration; backup and restore processes; network configuration; various system services; simple security administration; and updating and maintaining the system.

Prerequisite(s)/Corequisite(s): CSCI 1620 or CSCI 1840 or Instructor Permission.

CYBR 3370 SECURITY ADMINISTRATION - WINDOWS (3 credits)
This course covers topics a system administrator would encounter in their profession. The student will learn how a system administrator fulfills various organizational information resource management requirements using the Windows Operating System. Topics will include; installation; creating and maintaining file systems; user and group administration; backup and restore processes; network configuration; various system services; simple security administration; and updating and maintaining the system.

Prerequisite(s)/Corequisite(s): CSCI 1620 or CSCI 1840 or Instructor Permission.

CYBR 3450 NATURAL LANGUAGE PROCESSING (3 credits)
The course will provide overview of the topics in natural language processing such as word and sentence tokenization, syntactic parsing, semantic role labeling, text classification. We will discuss fundamental algorithms and mathematical models for processing natural language, and how these can be used to solve practical problems. We will touch on such applications of natural language processing technology as information extraction and sentiment analysis. (Cross-listed with CSCI 3450).

Prerequisite(s)/Corequisite(s): CSCI 2030; Co-requisite: CSCI 3320; Students should be comfortable w/ scripting (Python will be the language extensively used in natural language processing tools including NLTK). Not open to non-degree graduate students.

CYBR 3570 CRYPTOGRAPHY (3 credits)
The course will provide a broad overview of the concepts, fundamental ideas, vocabulary, and literature base central to the study and development of cryptography and cryptanalysis. This course will explore historical development of cryptography, as well as methods used to defeat it. In addition, the course will cover the mathematical foundations of cryptography today, as well as some current uses of such cryptography, such as public key infrastructures, the Internet Key Exchange protocol, and more.

Prerequisite(s)/Corequisite(s): CSCI 3320 or ISQA 3300. Not open to non-degree graduate students.

CYBR 3600 INFORMATION SECURITY, POLICY AND AWARENESS (3 credits)
This course will cover the planning and development for information governance, security policies and procedures, and security awareness. (Cross-listed with CIST 3600)

Prerequisite(s)/Corequisite(s): CIST 2100; CIST 3110, which may be taken concurrently.

CYBR 4000 CENTER OF ACADEMIC EXCELLENCE-CYBER OPERATIONS COMPLETION CERTIFICATE (0 credits)
This course is utilized to provide a specific designation for students that have completed the Center of Academic Excellence - Cyber Operations coursework. It is a zero credit hour class used to designate the completion of this focus area in the cybersecurity curriculum.

Prerequisite(s)/Corequisite(s): Instructor Permission. The program committee will work w/ the UG advisors to verify that the student has fulfilled the requirements for this designation. If the student has fulfilled (or will soon) all the requirements, they may register for this class.

CYBR 4360 FOUNDATIONS OF INFORMATION ASSURANCE (3 credits)
Contemporary issues in computer security, including sources for computer security threats and appropriate reactions; basic encryption and decryption; secure encryption systems; program security, trusted operating systems; database security, network and distributed systems security, administering security; legal and ethical issues. (Cross-listed with CYBR 8366, CSCI 8366)

Prerequisite(s)/Corequisite(s): CSCI 3320 or CSCI 8325 OR ISQA 3300 OR By instructor permission

CYBR 4380 COMPUTER AND NETWORK FORENSICS (3 credits)
Computer forensics involves the preservation, identification, extraction and documentation of computer evidence stored on a computer. This course takes a technical, legal, and practical approach to the study and practice of incident response, computer forensics, and network forensics. Topics include legal and ethical implications, duplication and data recovery, steganography, network forensics, and tools and techniques for investigating computer intrusions. This course is intended as a second course in information assurance for undergraduate students as well as other qualified students. It is also intended as a foundation course for graduate digital forensics studies. (Cross-listed with CSCI 4380, CYBR 8386)

Prerequisite(s)/Corequisite(s): CYBR 1100, CIST 3600, CSCI 3550 or ISQA 3400, CYBR 3350 or CYBR 3370; or instructor permission.
**CYBR 4430 QUANTUM COMPUTING AND CRYPTOGRAPHY (3 credits)**
The course aims at understanding the exciting concepts behind quantum computing and quantum cryptography. The course will introduce the principles of qubits, superposition, entanglement, teleportation, measurement, quantum error correction, quantum algorithms such as quantum Fourier transformation, Shor’s algorithm and Grover’s algorithm, quantum key exchange, quantum encryption, and secure quantum channels that built using these principles. We will discuss the security definitions and protocols within the quantum realm. We will discuss what advantages quantum computing and cryptography offers compared to classical computing and cryptography and limitations thereof. It will cover the integration of quantum cryptography into existing public key infrastructure. The students will come out with a working understanding of the field of quantum computing and quantum cryptography. During the course students will also implement several of the quantum algorithms. (Cross-listed with CYBR 8436)

**Prerequisite(s)/Corequisite(s):** Co-requisites: CYBR 3570 or CSCI 4560; or Instructor permission.

**CYBR 4440 INDUSTRIAL CONTROL SYSTEM SECURITY (3 credits)**
The objective of this course is to research vulnerabilities into, and provide guidance for securing, industrial control systems (ICS). ICS is a general term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system items such as Programmable Logic Controllers (PLC). The student will learn to identify network and device vulnerabilities and potential countermeasures to these weaknesses. (Cross-listed with CYBR 8446)

**Prerequisite(s)/Corequisite(s):** CSCI 3550.

**CYBR 4450 HOST-BASED VULNERABILITY DISCOVERY (3 credits)**
The class will cover security issues at an implementation and hardware level. The students will learn assembly language and the use of a reverse assembler and debugger. This will allow the student to analyze various packing algorithms for computer viruses, the viruses themselves, operating system hooking, fuzzing, and other machine code, host-based exploits. The class will be using both Windows and Linux as operating systems. (Cross-listed with CYBR 8456.)

**Prerequisite(s)/Corequisite(s):** Permission of the instructor and CSCI 3710.

**CYBR 4460 NETWORK-BASED VULNERABILITY DISCOVERY (3 credits)**
The course is an advanced class in which the students learn various techniques for testing for and identifying security flaws in network software and web applications. Internet technologies such as HTTP, DNS, DHCP, and others are examined in the context of cyber security. Students are expected to participate in numerous hands-on experiments related to Information Assurance with respect to web technologies. (Cross-listed with CYBR 8466)

**Prerequisite(s)/Corequisite(s):** Instructor Permission

**CYBR 4450 COMPUTER SECURITY MANAGEMENT (3 credits)**
The purpose of this course is to integrate concepts and techniques from security assessment, risk mitigation, disaster planning, and auditing to identify, understand, and propose solutions to problems of computer security and security administration. (Cross-listed with CIST 4540, CYBR 8546, ISQA 8546)

**Prerequisite(s)/Corequisite(s):** IASC 4360 or permission of the instructor.

**CYBR 4580 CERTIFICATION AND ACCREDITATION OF SECURE SYSTEMS (CAPSTONE) (3 credits)**
This is the BSIA capstone course where students extend and apply their knowledge in defining, implementing, and assessing secure information systems. Students will demonstrate their ability to specify, apply, and assess different types of countermeasures at different points in the enterprise with a special focus on system boundaries. Students will complete and defend a Certification and Accreditation package.

**Prerequisite(s)/Corequisite(s):** CIST 3600 or CYBR 3600; CIST 4360; CYBR 3350 or CYBR 3370; and CIST 4540 or CYBR 4540 may be taken prior to or concurrently. Not open to non-degree graduate students.

**CYBR 4950 INTERNSHIP IN INFORMATION ASSURANCE (1-3 credits)**
The course provides a format for an Information Assurance student to work with a local or national industry partner in a cyber security oriented position, and to receive credit for this practical experience. The internship may or may not be a paid position, but will definitely be directly related to Information Assurance. The class is proposed and organized by the student, with participating faculty supervising and input provided by the industry partner.

**Prerequisite(s)/Corequisite(s):** Instructor Permission

**CYBR 4980 SPECIAL TOPICS IN INFORMATION ASSURANCE (1-3 credits)**
The course provides a format for exploring advanced research areas for undergraduate students in Information Assurance and related fields. Specific topics vary, in keeping with research interests of faculty and students. Examples include applied data mining, mobile security, web services and applications, vulnerability assessments, cloud computing security, and other issues in Information Assurance research. (Cross-listed with CYBR 8986)

**Prerequisite(s)/Corequisite(s):** Instructor Permission

**CYBR 4990 INDEPENDENT STUDY IN INFORMATION ASSURANCE (1-3 credits)**
The course provides a format for exploring advanced research areas for undergraduate students in Information Assurance and related fields. The class is designed for students that would like to explore specific Information Assurance topics at a greater depth, or topics which are not currently a part of the IA curriculum. The class is proposed and organized by the student, with participating faculty mentoring.

**Prerequisite(s)/Corequisite(s):** Instructor Permission

**CYBR 8000 CENTER OF ACADEMIC EXCELLENCE-CYBER OPERATIONS COMPLETION CERTIFICATE (0 credits)**
This course is utilized to provide a specific designation for students that have completed the Center of Academic Excellence - Cyber Operations coursework. It is a zero credit hour class used to designate the completion of this focus area in the cybersecurity curriculum.

**Prerequisite(s)/Corequisite(s):** Instructor Permission. The program committee will work with the UG advisors to ascertain that the student has fulfilled all requirements for this designation-if he/she has or will within the last semester, they will be allowed to register for this class.

**CYBR 8080 SPECIAL TOPICS IN INFORMATION ASSURANCE (1-6 credits)**
The course provides a format for exploring advanced research areas for graduate students in Information Assurance and related fields. Specific topics vary, in keeping with research interests of faculty and students. Examples include applied data mining, mobile security, web services and applications, vulnerability assessments, cloud computing security, and other issues in Information Assurance research.

**Prerequisite(s)/Corequisite(s):** Instructor Permission.
**CYBR 8366 FOUNDATIONS OF INFORMATION ASSURANCE (3 credits)**

Contemporary issues in computer security, including sources for computer security threats and appropriate reactions; basic encryption and decryption; secure encryption systems; program security, trusted operating systems; database security, network and distributed systems security, administering security; legal and ethical issues. (Cross-listed with CYBR 4360, CSCI 8366)

Prerequisite(s)/Corequisite(s): CSCI 3320 or CSCI 8325 OR ISQA 3300 OR By instructor permission

**CYBR 8386 COMPUTER AND NETWORK FORENSICS (3 credits)**

Computer forensics involves the preservation, identification, extraction and documentation of computer evidence stored on a computer. This course takes a technical, legal, and practical approach to the study and practice of incident response, computer forensics, and network forensics. Topics include legal and ethical implications, duplication and data recovery, steganography, network forensics, and tools and techniques for investigating computer intrusions. This course is intended as a second course in information assurance for undergraduate students as well as other qualified students. It is also intended as a foundation course for graduate digital forensics studies. (Cross-listed with CYBR 4380, CSCI 4380)

Prerequisite(s)/Corequisite(s): CYBR 1100, CIST 3600, CSCI 3500 or ISQA 3400, CYBR 3350 or CYBR 3370; or instructor permission.

**CYBR 8410 DISTRIBUTED SYSTEMS AND NETWORK SECURITY (3 credits)**

The course aims at understanding the issues surrounding data security, integrity, confidentiality and availability in distributed systems. Further, we will discuss various network security issues, threats that exist and strategies to mitigate them. This course will cover topics in cryptography, public key infrastructure, authentication, hashing, digital signatures, ARP protection, IP and IPSEC, IP Tables, SSL/TLS, firewalls, etc. (Cross-listed with CSCI 8410)

Prerequisite(s)/Corequisite(s): IASC 8366 or equivalent(s); or instructor permission. Not open to non-degree graduate students.

**CYBR 8420 SOFTWARE ASSURANCE (3 credits)**

Software assurance is a reasoned, auditable argument created to support the belief that the software will operate as expected. This course is an intersection of knowledge areas necessary to perform engineering activities or aspects of activities relevant for promoting software assurance. This course takes on a software development lifecycle perspective for the prevention of flaws. (Cross-listed with CSCI 8420)

Prerequisite(s)/Corequisite(s): CSCI 4830 or CSCI 8836 OR by permission of the Instructor. Not open to non-degree graduate students.

**CYBR 8436 QUANTUM COMPUTING AND CRYPTOGRAPHY (3 credits)**

The course aims at understanding the exciting concepts behind quantum computing and quantum cryptography. The course will introduce the principles of qubits, superposition, entanglement, teleportation, measurement, quantum error correction, quantum algorithms such as quantum Fourier transformation, Shor’s algorithm and Grover’s algorithm, quantum key exchange, quantum encryption, and secure quantum channels that built using these principles. We will discuss the security definitions and protocols within the quantum realm. We will discuss what advantages quantum computing and cryptography offers compared to classical computing and cryptography and limitations thereof. It will cover the integration of quantum cryptography into existing public key infrastructure. The students will come out with a working understanding of the field of quantum computing and quantum cryptography. During the course students will also implement several of the quantum algorithms. (Cross-listed with CYBR 4430)

Prerequisite(s)/Corequisite(s): Co-requisites: CYBR 3570 or CSCI 4560; or Instructor permission

**CYBR 8440 SECURE SYSTEMS ENGINEERING (3 credits)**

This course takes a global risk-based view of the process of defining, verifying, validating and continuously monitoring secure information systems. The course will investigate a number of secure system solutions, starting with the definition of the system security needs, and tracing through methods of verification and validation of security controls, as well as ways to continuously monitor the corresponding assurances. (Cross-listed with CSCI 8440)

Prerequisite(s)/Corequisite(s): CSCI 8366 or IASC 8366.

**CYBR 8446 INDUSTRIAL CONTROL SYSTEM SECURITY (3 credits)**

The objective of this course is to research vulnerabilities into, and provide guidance for securing, industrial control systems (ICS). ICS is a general term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system items such as Programmable Logic Controllers (PLC). The student will learn to identify network and device vulnerabilities and potential countermeasures to these weaknesses. (Cross-listed with CYBR 4440)

Prerequisite(s)/Corequisite(s): CSCI 3550.

**CYBR 8450 APPLIED CRYPTOGRAPHY (3 credits)**

In this course we will implement stream and block ciphers in different modes, public key algorithms, hash functions, message authentication codes, random number generators, etc. Along the way we will also explore weaknesses of these algorithms and implement well-known attacks on them. We will also solve crypto challenges and puzzles. This is a hand-on course and will require programming proficiency. The preferred language will be Python; you can, however, use other object oriented languages.

Prerequisite(s)/Corequisite(s): CSCI 2030, CSCI 3320, CYBR 3570 or equivalent or Instructor Permission.

**CYBR 8456 HOST-BASED VULNERABILITY DISCOVERY (3 credits)**

The class will cover security issues at an implementation and hardware level. The students will learn assembly language and the use of a reverse assembler and debugger. This will allow the student to analyze various “packing” algorithms for computer viruses, the viruses themselves, operating system “hooking”, “fuzzing”, and other machine code, host-based exploits. The class will be using both Windows and Linux as operating systems. (Cross-listed with CYBR 4450.)

Prerequisite(s)/Corequisite(s): Permission of the instructor and CSCI 3710.

**CYBR 8460 SECURITY OF EMBEDDED SYSTEMS (3 credits)**

An embedded system is some combination of computer hardware and software, either fixed in capability or programmable, which is specifically designed for a particular function. Industrial machines, automobile electronic systems, medical equipment, cameras, household appliances, airplanes, vending machines, cellular phones and PDAs are among the myriad possible hosts of an embedded system. This class concerns itself with the security aspects of these often computationally restricted computing platforms

Prerequisite(s)/Corequisite(s): IASC 8366, CYBR 4450 or CYBR 8456.

**CYBR 8466 NETWORK-BASED VULNERABILITY DISCOVERY (3 credits)**

The course is an advanced class in which the students learn various techniques for testing for and identifying security flaws in network software and web applications. Internet technologies such as HTTP, DNS, DHCP, and others are examined in the context of cyber security. Students are expected to participate in numerous hands-on experiments related to Information Assurance with respect to web technologies. (Cross-listed with CYBR 4460)

Prerequisite(s)/Corequisite(s): Instructor Permission
CYBR 8470 SECURE WEB APPLICATION DEVELOPMENT (3 credits)
Web applications are pervasive fixtures of 21st century culture. Web application security is an inclusive, amorphous, term that spans application level security, i.e. ensuring high level code cannot be exploited, server level security, i.e. ensuring server resources such as databases and file systems cannot be exploited, and network security, i.e. ensuring unauthorized parties cannot access a server or tamper with user sessions. This course cross-cuts the web application security concepts across the different categories above and takes a heavily hands-on approach to introduce students to the world of secure web app. design and development.
Prerequisite(s)/Corequisite(s): Instructor Permission

CYBR 8546 COMPUTER SECURITY MANAGEMENT (3 credits)
The purpose of this course is to integrate concepts and techniques from security assessment, risk mitigation, disaster planning, and auditing to identify, understand, and propose solutions to problems of computer security and security administration. (Cross-listed with CIST 4540, CYBR 4540, ISQA 8546)
Prerequisite(s)/Corequisite(s): IASC 4360 or permission of the instructor.

CYBR 8570 INFORMATION SECURITY POLICY AND ETHICS (3 credits)
The course will cover the development and need for information security policies, issues regarding privacy, and the application of computer ethics. (Cross-listed with ISQA 8570)
Prerequisite(s)/Corequisite(s): CIST 2100 or BSAD 8030, or permission of instructor.

CYBR 8900 INDEPENDENT STUDY IN INFORMATION ASSURANCE (1-3 credits)
The course provides a format for exploring advanced research areas for graduate students in Information Assurance and related fields. The class is designed for students that would like to explore specific Information Assurance topics at a greater depth, or topics that are not currently a part of the IA curriculum. The class is proposed and organized by the student, with participating faculty mentoring.
Prerequisite(s)/Corequisite(s): Instructor Permission

CYBR 8910 INTERNSHIP (1-3 credits)
The purpose of this course is to provide the students with an opportunity for practical application and further development of knowledge and skills acquired in the MS in CyberSecurity (CYBR) program. The internship gives students professional work experience and exposure to the challenges and opportunities faced by IT professionals in the workplace.
Prerequisite(s)/Corequisite(s): Students must have completed a minimum of 12 credit hours towards the MS in CYBR program. Instructor permission is required to register. Not open to non-degree graduate students.

CYBR 8950 GRADUATE CAPSTONE IN INFORMATION ASSURANCE (3 credits)
This is the graduate capstone course where students extend and apply their knowledge in defining, implementing, and assessing secure information systems. Students will demonstrate their ability to specify, apply, and assess different types of countermeasures at different points in the enterprise with a special focus on system boundaries. Students will complete and defend a Certification and Accreditation package. This course is intended for graduate students in the MS in IA degree program, coursework option, that are close to graduation (see prerequisites). This course replaces the MS in IA comprehensive examination requirement.
Prerequisite(s)/Corequisite(s): CYBR 8366, CYBR 8410, and CYBR 8456 and concentration area (systems or management and policy). Students must have 6 credit hours or less left in the program.

CYBR 8986 SPECIAL TOPICS IN INFORMATION ASSURANCE (1-3 credits)
The course provides a format for exploring advanced research areas for undergraduate students in Information Assurance and related fields. Specific topics vary, in keeping with research interests of faculty and students. Examples include applied data mining, mobile security, web services and applications, vulnerability assessments, cloud computing security, and other issues in Information Assurance research. (Cross-listed with CYBR 4980)
Prerequisite(s)/Corequisite(s): Instructor Permission.

CYBR 8990 THESIS IN INFORMATION ASSURANCE (1-6 credits)
A research project, designed and executed under the supervision of the chair and approval by members of the graduate student's thesis advisory committee. In this project the student will develop and perfect a number of skills including the ability to design, conduct, analyze and report the results in writing (i.e., thesis) of an original, independent scientific investigation.
Prerequisite(s)/Corequisite(s): Instructor Permission.